ZMW AF

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Charles C. Brackett : **Account No.: 07-0845**

Serial No.: 09/667,742 : **Order No.: 15-UL-5580**

Filed: September 22, 2000

Title: ULTRASOUND IMAGING SYSTEM HAVING VIRUS PROTECTION

Hon. Commissioner for Patents
Alexandria, VA 22313

DEPOSIT ACCOUNT ORDER FORM

Sir:

The Applicant requests that the fee for filing an appeal brief, in the amount of $500.00, be charged to Deposit Account No. 07-0845 in the above-referenced patent application. The name and address of the Depositer is:

GE Medical Systems
P.O. Box 414
Milwaukee, WI 53201
Attn.: Pete Vogel

Respectfully submitted,

December 8, 2006
Date

Dennis M. Flaherty
Reg. No. 31,159
Ostrager Chong Flaherty & Broitman P.C.
250 Park Avenue, Suite 825
New York, NY 10177-0899
Tel. No.: 212-681-0600

Atty. Docket: 15-UL-5580

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

In re Application of:

Charles C. Brackett : Group Art Unit: 2134

Serial No.: 09/667,742 : Examiner: Heneghan, M.E.

Filed: September 22, 2000

Title: ULTRASOUND IMAGING SYSTEM HAVING VIRUS PROTECTION

Hon. Commissioner for Patents
Alexandria, VA 22313

APPEAL BRIEF

A Notice of Appeal was filed in the above-identified application on October 16, 2006. A Pre-Appeal Brief Request for Review was filed concurrently therewith. On November 8, 2006, a Notice of Panel Decision from Pre-Appeal Brief Review was mailed in which the time for filing an appeal brief was reset to be one month from the mailing of the decision, i.e., December 8, 2006. Accordingly, no fee for any extension of time is required.

The fee for filing an appeal brief, in the amount of $500.00, should be charged to Deposit Account No. 07-0845.

1. Real Party in Interest

GE Medical Systems Global Technology Company, LLC, having offices in Waukesha, Wisconsin, is the assignee and owner of 100% interest in this patent application and therefore is the real party in interest.

2. Related Appeals and Interferences

The appellant, appellant's legal representative and the assignee do not know of any other appeals, interferences or judicial proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

3. Status of Claims

Claims 1-5, 8-13 and 30-36 are pending; claims 6, 7 and 14-29 have been canceled. The Final Rejection of claims 1-5, 8-13 and 30-36 is being appealed.

4. Status of Amendments

No Amendment was filed after the Final Rejection mailed on July 20, 2006.

5. Summary of Claimed Subject Matter

This application has two independent claims 1 and 30. Both independent claims are involved in this appeal.

Claim 1. The subject matter recited in independent claim 1 is an ultrasound imaging system comprising:

an image acquisition subsystem for acquiring frames of image data (transducer array 2, beamformer 4 and B-mode processing chain 6 in FIG. 1; see also p. 5, ll. 16-32);

system memory storing said acquired frames of image data and operating instructions (scan converter 10 and host computer 20 in FIG. 1; video memory 11 and host computer 20 in FIG. 2; see also p. 6, ll. 2-4 and 28-31; p. 7, ll. 18-20);

a display subsystem for displaying images derived from said acquired frames of image data (display monitor 18 in FIGS. 1 and 2; see also p. 6, ll. 11-13);

a display processor for controlling said display subsystem to display frames of image data (video processor 14 in FIGS. 1 and 2; see also p. 6, ll. 9-11);

a hard disk (item 21 in FIGS. 2 and 3) storing frames of image data (see p. 6, ll. 26 and 27), said operating instructions (see p. 6, ll. 29 and 30) and a registry file containing encrypted data representing a list of all processes that are approved by the system manufacturer or service provider to run on the imaging system (see p. 4, ll. 7 and 8; p. 9, ll. 27-30);

an operating system (item 36 in FIG. 3) that copies said operating instructions from said hard disk to said system memory when the imaging system is powered up (p. 6, ll. 29-31; p. 9, ll. 18-20); and

a host computer (item 20 in FIGS. 1 and 2) programmed to control said image acquisition subsystem and said display subsystem in accordance with operating instructions transferred from said hard disk to said system memory (p. 6, ll. 28-31), and further programmed with first and second computer virus protection features, said first computer virus protection feature comprising means (virus scanning software 32 in FIG. 3; see p. 7, ll. 7, ll. 31-34) for detecting a file having an attribute of a computer virus before said file is installed on

said hard disk, and said second computer virus protection feature comprising means for monitoring an application program to be executed by said operating system but not yet copied from said hard disk to said system memory, said monitoring means comprising means for decrypting said encrypted data in said registry file (encrypter/decrypter 39 in FIG. 4; see p. 10, ll. 9-12) and means for searching said decrypted data for an entry matching the identifier received from said operating system identifying a starting process of said application program to be executed by said operating system (virus protection monitor 38 in FIG. 4; see p. 10, ll. 12-15).

Claim 30. The subject matter recited in independent claim 30 is an ultrasound imaging system comprising all of the same elements recited in claim 1, except for the "means for detecting a file having an attribute of a computer virus before said file is installed on said hard disk". Accordingly, support for the limitations recited in claim 30 in the specification and drawings is the same as cited above.

6. Ground of Rejection to Be Reviewed on Appeal

In ¶ 3 of the Final Rejection, claims 1, 4, 8, 9, 11-13, 30-32, and 34-36 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hiyama (US 6,269,379) in view of McGee (US 6,694,434) and further in view of Lang (US 5,191,611) and Hile (US 5,319,776).

7. Argument

The Appellant believes that the Final Rejection is clearly erroneous for the following reasons.

Independent claims 1 and 30 each recite "means for decrypting said encrypted data in said registry file and means for searching said decrypted data for an entry matching the identifier received from said operating system identifying a starting process of said application program to be executed by said operating system."

The Final Rejection cites McGee as teaching registry information that is digitally signed using a private key and then authenticated (i.e., decrypted) using a public key. However, this feature in McGee is different than Appellant's claimed registry. Appellant's claimed invention includes "a registry file containing encrypted data representing a list of all processes that are approved by the system manufacturer or service provider to run on the imaging system". This registry does not contain encrypted data that is specific to a particular user, but rather contains encrypted data for processes "approved by the system manufacturer or service provider" regardless of who the user is. In other words, all that matters is whether the process is approved, not whether the user of the process is approved. If, as proposed by McGee, the system were to be capable of allowing a user to digitally sign the application registration data using a private signing key, the system would then need to decrypt that data using "the

user's public signing key" (see McGee, col. 5, lines 10-12). That "user's" public signing key is specific to the user. Public keys are often stored on public key servers. Each user would have his own public signing key stored in the public key server or registry, if you will. This is clearly different from Appellant's claimed invention, wherein the process to be executed is compared to data obtained by decrypting encrypted data stored in a registry, that encrypted data representing approved processes. Unlike McGee, Appellant's claimed invention does not require the use of encrypted data that identifies the user. Instead the claimed invention authenticates the requested process to be executed using encrypted data that identifies approved processes.

Furthermore, independent claims 1 and 30 each recite that the host computer is programmed to decrypt the encrypted data in the registry and then search that decrypted data for an entry matching an identifier received from the operating system identifying a starting process of an application program to be executed by the operating system. The McGee patent does not disclose this step, but rather discloses that the computing unit "generates a hash value of a requesting application and evaluates whether the generated hash value matches the centralized registration list" (see McGee, col. 5, lines 17-20). There is no disclosure that the entries in the centralized registration list are decrypted. Furthermore, the digital signature of McGee is an encryption of a hash value derived from a list of hash values generated from the executable files.

Conversely, the decryption of that digital signature will be the hash value derived from the list (i.e., multiplicity) of hash values and is not the hash value of any particular executable file. McGee teaches that the execution of files is monitored by comparing the hash values stored in the registry list to the hash value generated from the file to be executed (see McGee, col. 4, lines 25-27). If there is a match, the application is granted execution privileges (see McGee, col. 5, lines 6-7).

More specifically, McGee uses hash values generated using "one-way hash functions", as stated at col. 7, line 28 and col. 8, line 53. A hash function H is a transformation that takes a variable-size input m and returns a fixed-size string, which is called the hash value h (that is $h = H(m)$. One basic requirement of a cryptographic hash function is that it be "one-way". A hash function is said to be "one-way" if it is hard to invert, meaning that given a hash value h, it is computationally unfeasible to find some input x such that $H(x) = h$. In other words, the one-way hash values disclosed by McGee are not decrypted and could not be decrypted, which is largely due to the fact that the hash values are generated by transforming a large domain into a small range, resulting in lost data that cannot be recovered by inverting the hash function.

Nor does the Lang patent disclose the key features that are missing from McGee. In particular, Lang does not disclose the use of a registry containing encrypted data representing

processes approved for execution on a computer. Instead, Lang discloses that a user can access encrypted directories of files by inputting an encrypted security identification code that identifies the user personally. The encrypted directory is then decrypted and then re-encrypted using the user's personal security key. Lang neither discloses nor suggests decrypting a registry of encrypted data representing approved processes and then comparing the decrypted data with the process requested by the user to find a match.

Accordingly, Appellant respectfully submits that neither McGee nor Lang discloses or suggests the monitoring means recited in claims 1 and 30. The Examiner does not assert that Hiyama or Hile disclose that feature either.

Secondly, a *prima facie* case of obviousness has not been shown because there is no motivation or suggestion to import the teachings of McGee into the image filing system of Hiyama, let alone into an ultrasound imaging system. The Examiner cites to a passage in Hiyama (see col. 8, lines 66 and 67) that teaches the use of a password to prevent unauthorized copying of any file during running of the operating system 82, thereby preventing the "invasion of [a] computer virus into a running application or other program". Since Hiyama has already solved the problem of preventing infection of his image filing system with a computer virus, there would be no need to incorporate the registration system of McGee to solve the same problem.

Accordingly, Appellant respectfully submits that claims 1 and 30 are not obvious in view of Hiyama, McGee, Lang and Hile.

The obviousness rejections set forth in ¶¶ 4 and 5 of the Final Rejection are based on the aforementioned combination of prior art as applied to claim 1 and/or 30 in combination with a fifth reference (namely, Yamamoto or Kisor). These rejections suffer from the same infirmities as those noted above vis-à-vis the Hiyama/McGee/Lang/Hile combination.

In view of the foregoing, Appellant submits that claims 1-5, 8-13 and 30-36 are patentable over the combination of prior art cited by the Examiner. Accordingly, it is respectfully requested that the Final Rejection be overturned and that this application be allowed.

Respectfully submitted,

December 8, 2006
Date

Dennis M. Flaherty
Reg. No. 31,159
Ostrager Chong Flaherty & Broitman P.C.
250 Park Avenue, Suite 825
New York, NY 10177-0899
Tel. No.: 212-681-0600

CERTIFICATE OF MAILING

The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Appeal Brief – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date set forth below.

December 8, 2006
Date

Dennis M. Flaherty

Claims Appendix

Claim 1: An ultrasound imaging system comprising:

an image acquisition subsystem for acquiring frames of image data;

system memory storing said acquired frames of image data and operating instructions;

a display subsystem for displaying images derived from said acquired frames of image data;

a display processor for controlling said display subsystem to display frames of image data;

a hard disk storing frames of image data, said operating instructions and a registry file containing encrypted data representing a list of all processes that are approved by the system manufacturer or service provider to run on the imaging system;

an operating system that copies said operating instructions from said hard disk to said system memory when the imaging system is powered up; and

a host computer programmed to control said image acquisition subsystem and said display subsystem in accordance with operating instructions transferred from said hard disk to said system memory, and further programmed with first and second computer virus protection features, said first computer virus protection feature comprising means for detecting a file having an attribute of a computer virus before said file is installed on said hard disk, and said second computer virus protection feature comprising means for monitoring an application program to be executed by said operating system but not yet copied from said hard disk to said system memory, said monitoring means comprising means for decrypting said encrypted data in said registry file and means for searching said decrypted data for an entry matching the identifier received from said operating system identifying a starting process of

said application program to be executed by said operating system.

Claim 2: The ultrasound imaging system as recited in claim 1, wherein said attribute is a checksum of said file.

Claim 3: The ultrasound imaging system as recited in claim 1, wherein said attribute is a size of said file.

Claim 4: The ultrasound imaging system as recited in claim 1, wherein said host computer is further programmed with:

means for actuating display of a graphical user interface by said display subsystem in response to detection of said file having an attribute of a computer virus, said graphical user interface comprising a virus alert and a virtual actuator; and

means for instructing said operating system to install said file in response to selection of said virtual actuator.

Claim 5: The ultrasound imaging system as recited in claim 4, further comprising a log of virus detection events, wherein said host computer is further programmed with means for logging an entry in said log in response to selection of said virtual actuator.

Claim 8: The ultrasound imaging system as recited in claim 1, wherein said host computer is further programmed with means for actuating display of a first graphical user interface by said display subsystem in response to detection that said starting process is not registered, said first graphical user interface comprising a virus alert and a virtual actuator.

Claim 9: The ultrasound imaging system as recited in claim 8, wherein said host computer is further programmed with means for instructing said operating system to kill said starting process in response to selection of said virtual actuator on said first graphical user interface.

Claim 10: The ultrasound imaging system as recited in claim 9, further comprising a log of virus detection events, wherein said host computer is further programmed with means for logging an entry in said log in response to selection of said virtual actuator on said first graphical user interface.

Claim 11: The ultrasound imaging system as recited in claim 9, wherein said host computer is further programmed with means for instructing said operating system to remove said application program from said hard disk in response to selection of said virtual actuator on said first graphical user interface.

Claim 12: The ultrasound imaging system as recited in claim 8, wherein said host computer is further programmed with:

means for actuating display of a second graphical user interface by said display subsystem in response to selection of said virtual actuator on said first graphical user interface, said second graphical user interface comprising a request for confirmation and a virtual actuator; and

means for adding information to said registry file for registering said application program in response to selection of said virtual actuator on said second graphical user interface.

Claim 13: The ultrasound imaging system as recited in claim 12, further comprising an encrypter arranged to encrypt

information sent from said host computer to said registry file on said hard disk.

Claim 30: An ultrasound imaging system comprising:

an image acquisition subsystem for acquiring frames of image data;

system memory storing said acquired frames of image data and operating instructions;

a display subsystem for displaying images derived from said acquired frames of image data;

a display processor for controlling said display subsystem to display frames of image data;

a hard disk storing frames of image data, said operating instructions and a registry file containing encrypted data representing a list of all processes that are approved by the system manufacturer or service provider to run on the imaging system;

an operating system that copies said operating instructions from said hard disk to said system memory when the imaging system is powered up; and

a host computer programmed to control said image acquisition subsystem and said display subsystem in accordance with operating instructions transferred from said hard disk to said system memory, and further programmed with means for monitoring an application program to be executed by said operating system but not yet copied from said hard disk to said system memory, said monitoring means comprising means for decrypting said encrypted data in said registry file and means for searching said decrypted data for an entry matching the identifier received from said operating system identifying a starting process of said application program to be executed by said operating system.

Claim 31: The ultrasound imaging system as recited in claim 30, wherein said host computer is further programmed with means for actuating display of a first graphical user interface by said display subsystem in response to detection that said starting process is not registered, said first graphical user interface comprising a virus alert and a virtual actuator.

Claim 32: The ultrasound imaging system as recited in claim 31, wherein said host computer is further programmed with means for instructing said operating system to kill said starting process in response to selection of said virtual actuator on said first graphical user interface.

Claim 33: The ultrasound imaging system as recited in claim 32, further comprising a log of virus detection events, wherein said host computer is further programmed with means for logging an entry in said log in response to selection of said virtual actuator on said first graphical user interface.

Claim 34: The ultrasound imaging system as recited in claim 32, wherein said host computer is further programmed with means for instructing said operating system to remove said application program from said hard disk in response to selection of said virtual actuator on said first graphical user interface.

Claim 35: The ultrasound imaging system as recited in claim 31, wherein said host computer is further programmed with:

means for actuating display of a second graphical user interface by said display subsystem in response to selection of said virtual actuator on said first graphical user interface, said second graphical user interface comprising a request for

confirmation and a virtual actuator; and

means for adding information to said registry file for registering said application program in response to selection of said virtual actuator on said second graphical user interface.

Claim 36: The ultrasound imaging system as recited in claim 35, further comprising an encrypter arranged to encrypt information sent from said host computer to said registry file on said hard disk.